the chili box

configuration guide

build: **2.1.7.3**

Chili Systems, Inc.

the chili box configuration guide

copyright notice

Copyright © 2001-2005 Chili Systems, Inc. All rights reserved.
Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format. “the chili box” is a trademark of Chili Systems, Inc.

Other product and company names mentioned herein can be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

limited warranty

Please refer to the chili box quick-start guide for Chili Systems, Inc.’s warranty policy. Technical Support is available between the hours of 8:00 AM and 9:00 PM Eastern Standard Time, Monday through Friday.

phone: 866•532•4454 x4
email: support@chilisystems.com

table of contents

COPYRIGHT NOTICE 3
TABLE OF CONTENTS 4
INTRODUCTION 5
DOMAIN NAME SYSTEM (DNS) 6
ADD DNS DOMAIN NAME 6
EDIT DNS DOMAIN NAME 7
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) 8
RESERVE IP ADDRESS 9
DHCP LEASES 10
NETWORK ADDRESS TRANSLATION (NAT) 11
ADD NEW ROUTE 12
FIREWALL 13
NEW PORT RULE 14
SORT PORT RULES 14
WEB PROXY 15
ADD BLOCK 16
ADD ALLOWANCE 17
FILESHARE 18
EDIT CHILI BOX WORKGROUP NAME 18
MANAGE USERS 19
MANAGE SHARES 21
USB BACKUP 23
MAIL 24
SERVER CONFIGURATION 24
MANAGE USERS 25
LIST CONFIGURATION 26
SPAM CONFIGURATION 27
VPN 28
GENERATE SECRET 28
ADD TUNNEL 29
EDIT TUNNEL 30
NETWORK SERVICES 31
STOP, RESTART, OR DISABLE SERVICE 31
HOW TO RESTART THE CHILI BOX 32
PREFERENCES 33
CHANGE PASSWORD 33
CHANGE NOTIFICATION 33
POP-UP RESTART REMINDERS 33
REMOTE ACCESS 34
REMOTE ADMINISTRATION 34
ENABLE CHILI SYSTEMS TECHNICAL SUPPORT 34
CHILI BOX MANAGERS 35
ADD CHILI BOX MANAGER 35
APPENDIX A: HOW TO CHOOSE A PASSWORD 36

introduction

The purpose of the configuration guide is to enable you to configure the more advanced features and services of the chili box, which include:

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)
- Firewall
- Web Proxy
- Fileshare
- USB Backup
- Mail
- VPN

This guide assumes you are familiar with the basic functionality and steps required to access the chili box management interface. If you are in need of assistance, please refer to the quick-start guide.

By default, an administrator account is created with access to ALL services. It is mentioned throughout this guide since it is always accessible; however, any of the steps on the following pages may be followed by any account with access to the appropriate service(s).

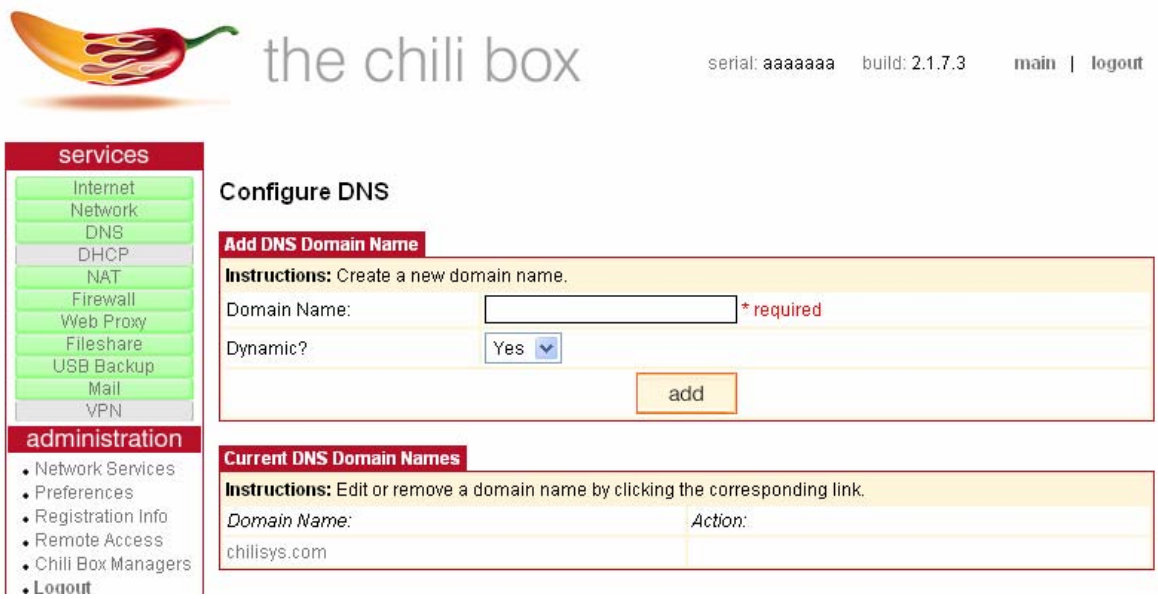
The chili box Web management interface is known as the GUI (Graphical User Interface) and is referred to as such throughout this document.

Domain Name System (DNS)

DNS allows a computer connected to the Internet to use a familiar name to access a Web site. For example, a user could enter www.google.com into a Web browser and the URL would be converted into an IP address by querying a DNS server.

The chili box comes with a robust DNS server that allows clients connected on the LAN interface to query the chili box for IP addresses without needing to leave the secure LAN environment. This enhances security since client computers do not need to query an outside server, which may have been compromised.

The chili box DNS management screen (shown below) can hold an unlimited number of internal domains for local resolution. Please note that the internal domain name, chilisys.com, cannot be deleted.



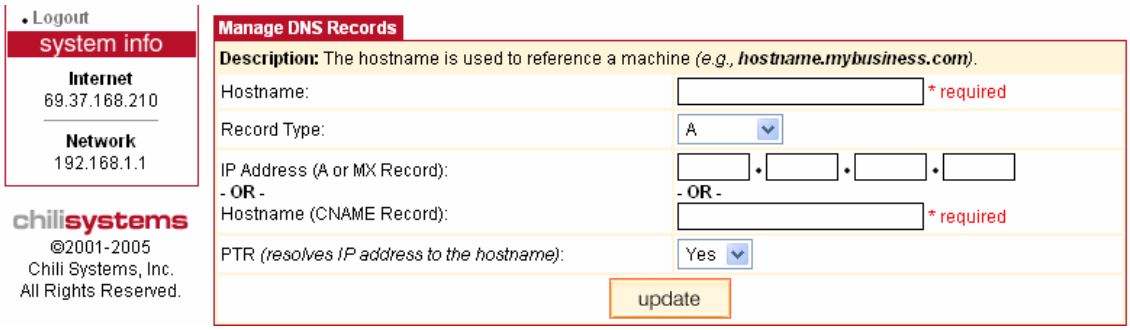
In addition, the chili box can provide Dynamic DNS capabilities to the LAN environment, allowing for DHCP to assign addresses to printers, desktops, and laptops. The DNS server will automatically record the name for local name to IP address resolution.

Add DNS Domain Name

1) Under “Add DNS Domain Name”, enter the “Domain Name”.
2) If you would like the domain name to also be updated via the LAN, leave the “Dynamic?” option as “Yes”; selecting “No” will only allow it to be updated manually.

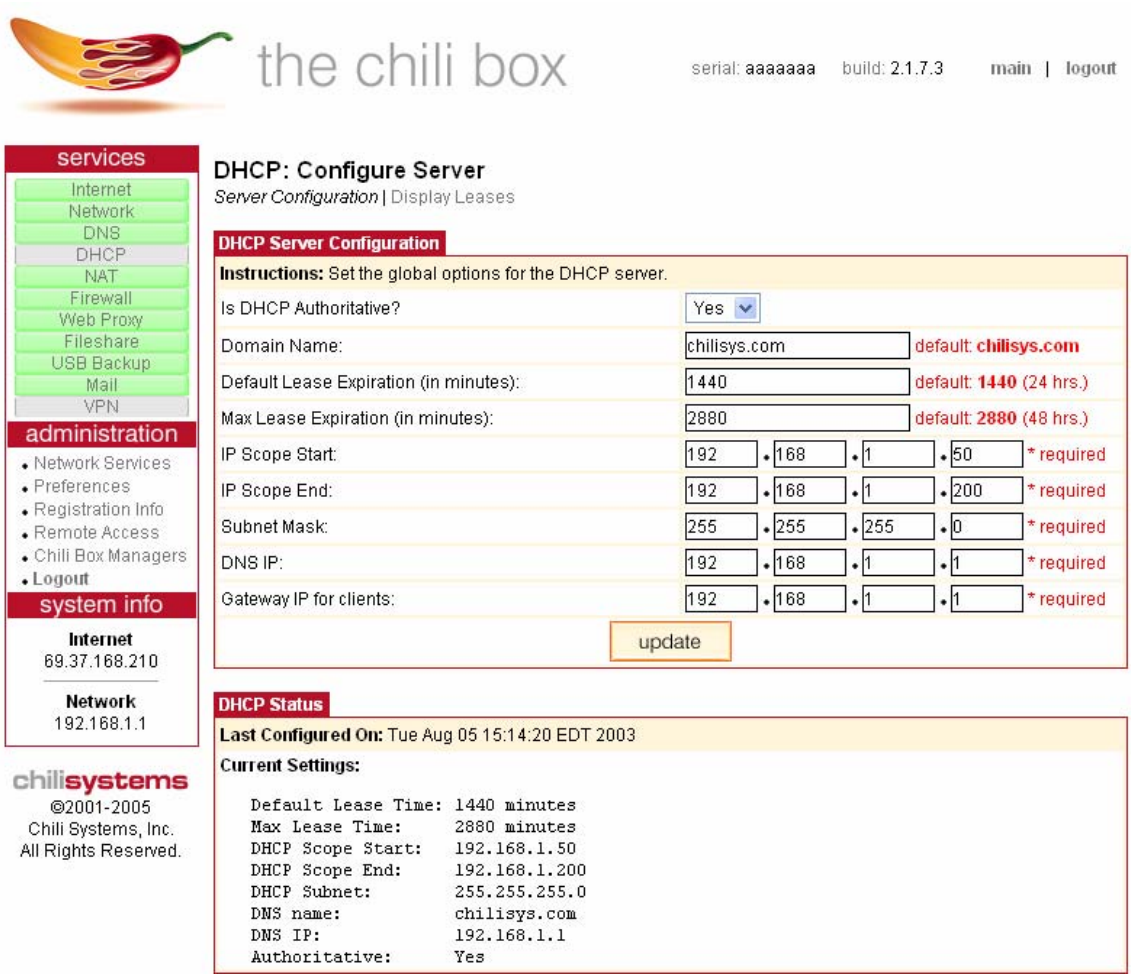
Edit DNS Domain Name

1) Under “Current DNS Domain Names”, click the domain name you wish to edit.
2) At the top of the page, under “Manage DNS Records”, enter the “Hostname” you wish to associate with the record, such as “www” for a Web site or “mail” for a Mail server.
3) Select the “Record Type” you would like to use:
   - “A” is the address record, which is not associated with mail, such as “www”
   - “MX” is the mail exchanger, which is only used for mail, such as “mail”
   - “CNAME” is similar to an alias, such as “www2.domain.com”
4) Depending on the type of record, enter the “IP Address” or “Hostname”:
   - “A” or “MX” use an IP address; enter it in the “IP Address” fields
   - “MX” or “CNAME” use a hostname; enter it in the “Hostname” field
5) Select if you would like to use a PTR, which is useful if you wish to find out the name of a user’s computer by doing a reverse lookup on the IP address.
6) Click ‘update’ when finished.



Dynamic Host Configuration Protocol (DHCP)

The chili box has a DHCP server, which can automatically assign IP addresses to computers on the LAN. This makes it much easier to administer, since you do not have to manually configure each client computer to access the network.



Is DHCP Authoritative? – The DHCP server on the chili box can be set as the "Authoritative" server on the LAN, the server that is responsible for providing IP addresses.

Domain Name – The domain name can be set for a LAN to assign it to clients requesting a DHCP address. If a host name has been set on the client, it will be added to the beginning of the LAN domain name. For example, if the host name was "office308pc" and the LAN domain name was "chilisys.com", the fully-qualified name after a successful DHCP lease would be "office308pc.chilisys.com".

Default Lease Expiration – This setting changes the amount of time a client computer will be assigned a leased IP address.

Max Lease Expiration – This setting assigns the maximum length in seconds that will be assigned to a lease.

IP Scope Start – Client computers can be assigned an IP address starting from this address.

IP Scope End – Client computers can only be assigned an IP address up to this number and no further.

Subnet Mask – Computers requesting an address will also be given this subnet mask to make them part of the overall network segment.

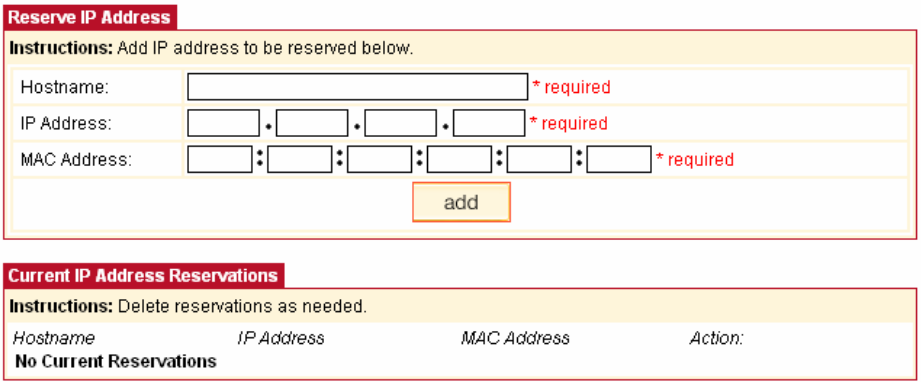
DNS IP – This setting will assign the DNS server for the LAN segment that the chili box is responsible for (by default this is usually the chili box's IP address).

Gateway IP for clients – If you wish, you may enter a separate internal IP address for client workstations to use. This will not affect the actual Gateway listed under "Internet" on the left.

Reserve IP Address

If you would like to specify a static IP address for a device on the network, such as a printer, you may reserve an IP address. This will ensure that the IP is not given out and will also allow users to reach the device by name.

1) Under "Reserve IP Address", enter the "Hostname".
2) Enter the static internal "IP Address".
3) Enter the "MAC Address"— this can be found on Windows 9x by running "winipcfg" and clicking 'More Info >>' and on Windows Me/NT/2000/XP by using the "ipconfig /all" command; it will be displayed on a printer by viewing the status display monitor.
4) Click 'add' when finished.



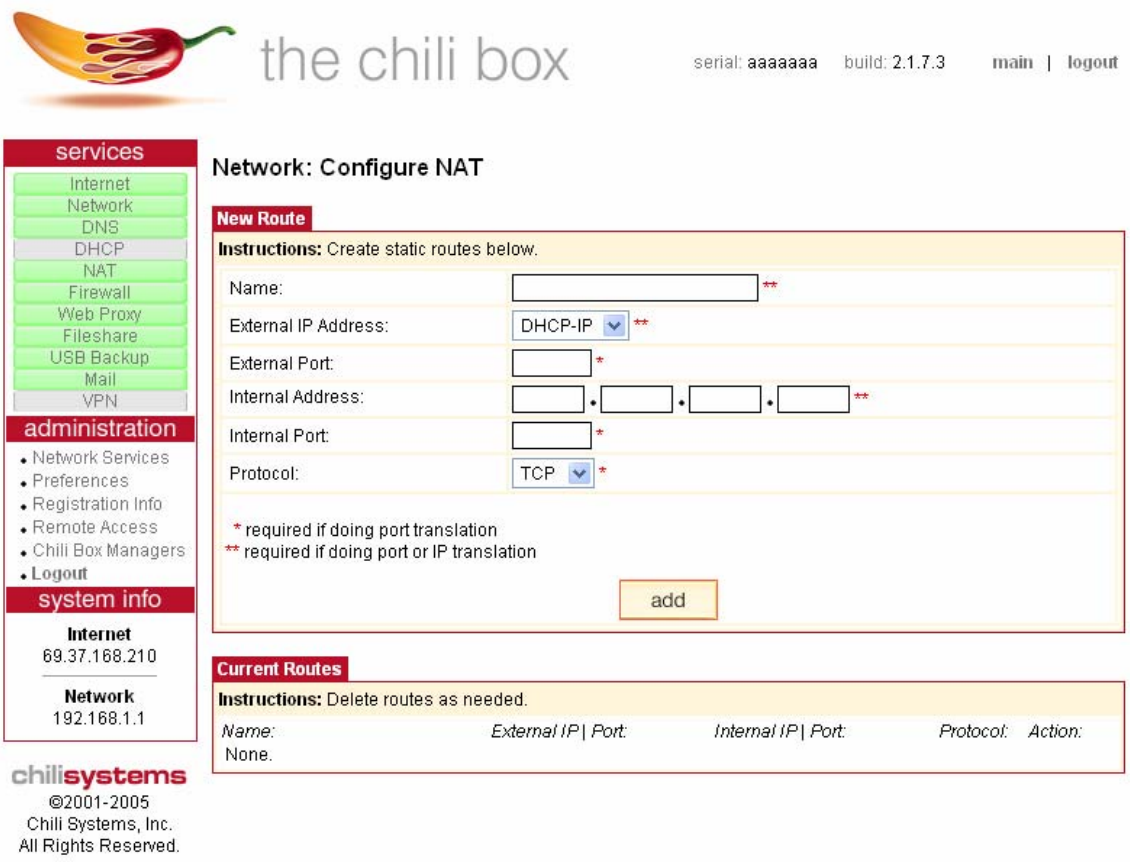
DHCP Leases

If you would like to view the current computers, printers, etc. connected to the chili box network, the corresponding names and internal IP addresses will be listed here.

Network Address Translation (NAT)

Network Address Translation (NAT) changes each LAN computer request for Internet access so that its IP address becomes the chili box's IP address. This allows the chili box to examine the packets coming from a remote computer, but the remote computer will think it's really communicating with the chili box. Since all packets must pass through the chili box to arrive at a host on the LAN, the chili box can drop any malicious traffic before it reaches the original host computer.

In addition, the chili box can expose a specific port from a computer inside the LAN to the Internet. This will allow a computer to offer services to the Internet such as e-mail, Web, and remote desktop while still being protected by the chili box.



Name – A description given to the NAT route to remember what it is for.

External IP Address – This setting is used to select the outside IP address that the NAT route will answer incoming requests from (please note that when using a dynamic address only "DHCP" can be selected).

External Port – This is the external port to expose to the Internet.

Internal IP Address – This setting selects the IP address on the LAN to connect the NAT route.

Internal Port – This is the internal port listening on the internal IP address specified above.

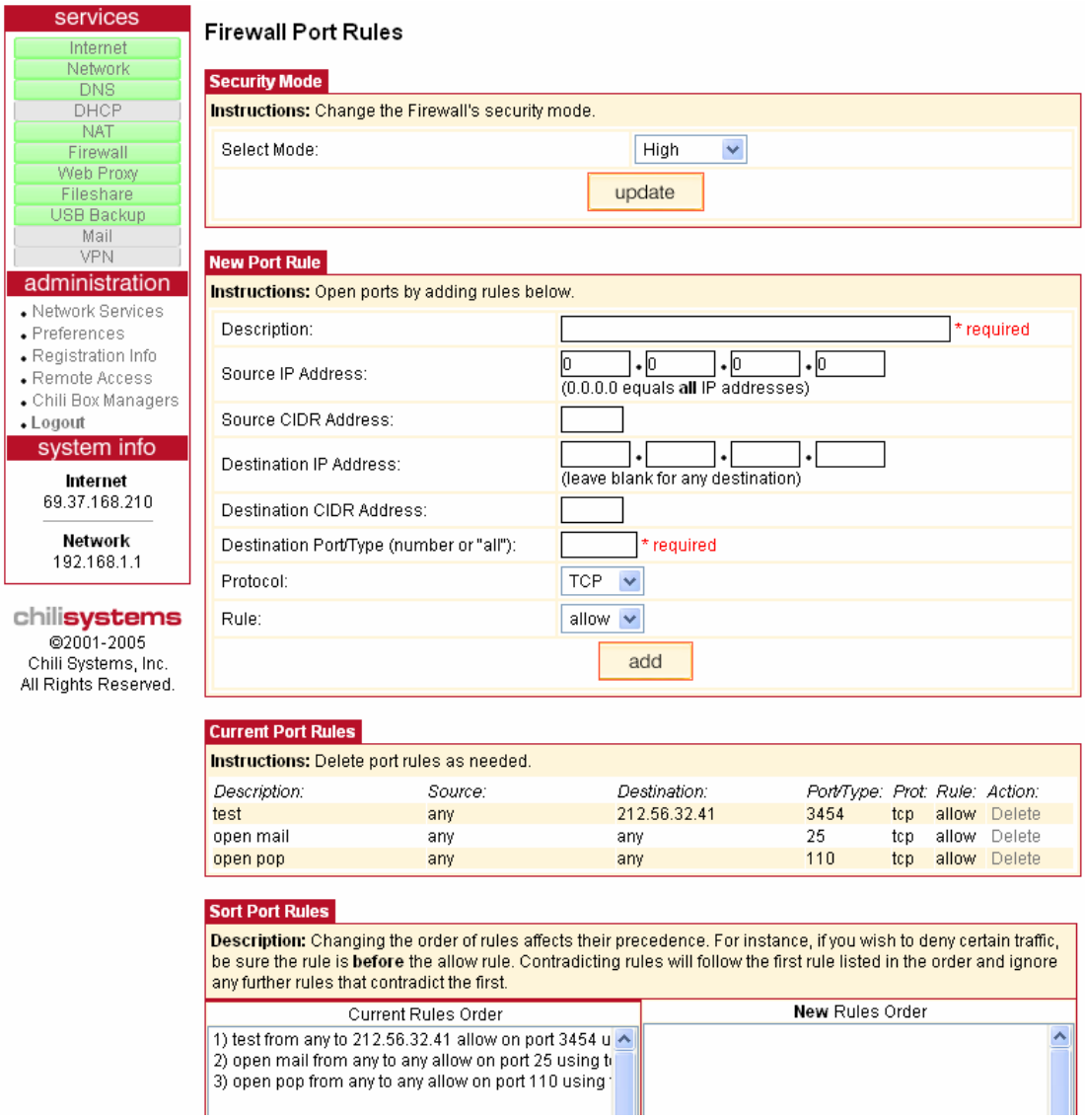
Protocol – Use this drop-down to select the protocol to map into the internal network.

Add New Route

1) Under “New Route”, enter the “Name” of the route.
2) Depending on how you configured the chili box, you may select to use “DHCP-IP” or one of your external IP addresses as the “External IP Address”.
3) Enter the “External Port” of the rule, which is used for the computer connecting through the chili box.
4) Enter the “Internal IP Address” of the client you would like to have access from.
5) Enter the “Internal Port” of the rule, which is configured in the “Firewall: Add New Port Rule” section, explained on the next page.
6) Enter the “Protocol” that the rule will use:
   - ”TCP” is a connection-oriented protocol, which requires a handshake
   - “UDP” is a connection-less protocol, which does not require a handshake
7) Click ‘add’ when finished.

Firewall

A firewall protects a network from the external network. This prevents unauthorized access to the internal network, since it blocks outsiders from viewing private data resources. In addition, when used with the proxy server, appropriate rules may be set up to control network users' privileges of and access to the Internet.



Description – An explanation given to the Firewall port rule for easy identification.

Source IP Address – This setting is used to select the outside IP address that the Firewall port rule will answer incoming requests from.

Source CIDR Address – Enter the source's CIDR address here, if necessary.

Destination IP Address – This setting is used to select the inside or outside IP address that the Firewall port rule will direct incoming requests to.

Destination CIDR Address – Enter the destination's CIDR address here, if necessary.

Destination Port/Type – This is the internal port number for TCP (e.g., SMTP is 25, POP3 is 110) or UDP, or type (ICMP) listening for the rule.

Protocol – Use this drop-down to select the protocol to map into the internal network.

Rule – Use this drop-down to select "allow" or "deny" to grant or block access, respectively.

New Port Rule

1) Under "New Port Rule", enter a "Description" of the port rule.
2) Enter the "Source IP Address" (please note that the default of 0.0.0.0 allows all IP addresses to use port rule).
3) Enter the "Destination IP Address" (leave blank for any destination).
4) Enter the Destination Port/Type" number, which is to be used as the internal port/type when adding a NAT route.
5) Enter the "Protocol" that the port rule will use:
   - "TCP" is a connection-oriented protocol, which requires a handshake
   - "UDP" is a connection-less protocol, which does not require a handshake
   - "ICMP" is a message control and error-reporting protocol, such as a Ping request
6) Select the "Rule" that you would like to use, either "allow" or "deny".
7) Click 'add' when finished.

Sort Port Rules

Once you have configured more than one Firewall port rule, you may follow the optional instructions below to change the precedence of the rules. This is useful if two rules exist that require a logical order to be followed. For example:

1) Web Traffic - deny using protocol tcp and ip 172.16.0.153 on port 80
2) Web Traffic - allow using protocol tcp and ip any on port 80

When the Firewall follows the above order, it denies access from 172.16.0.153 but allows access by all others. If the order were reversed, it would allow access by all and ignore the "deny" rule, which would render it useless. The current order of the rules is listed under "Current Rules Order".

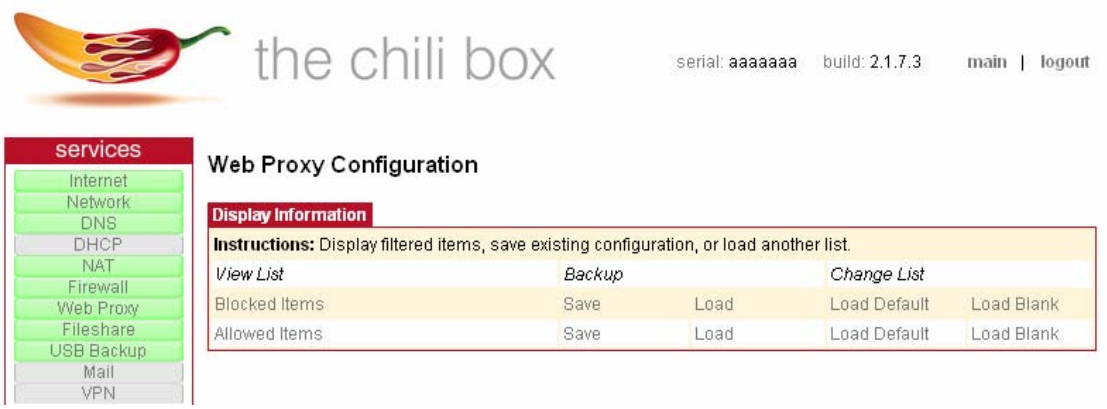
1) When you have decided on the precedence of the rules for the system to follow, click each rule once in the same order.
2) You will notice that the order will change under "New Rules Order"; if you wish to remove certain rules, simply select each and click 'Remove Value'.
3) Click 'Submit Values' when finished to save the changes.

Web Proxy

A Web proxy allows an administrator to control the site and content that all users are allowed or not allowed to view. The chili box uses a transparent proxy, which essentially means that each client's Web browser software does not need to be configured to use a proxy server. Everything is done transparently to the user, allowing you to control Internet usage at your own discretion.

You may configure blocks to filter by site names (e.g., playboy.com, whitehouse.com, etc.), or, if you wish to prohibit usage for numerous sites, by phrases (e.g., sex, xxx, etc.). Conversely, you may configure allowances by site names (e.g., google.com, whitehouse.gov) or phrases (e.g., Essex). If a block and allowance conflict with each other, the allowance will take precedence.

Since the Web Proxy filter is based on the URL or keyword and is not case sensitive, it can easily be configured to block or allow file extensions, such as MPG, MOV, MP3, AVI, etc.



Blocked Items – View current sites and phrases that are denied from being accessed.

Allowed Items – View current sites and phrases that are granted to be accessed.

Save – Back up current configuration.

Load – Open a previously saved configuration.

Load Default – Revert to factory default listing.

Load Blank – Clear existing entries so listing is completely empty.

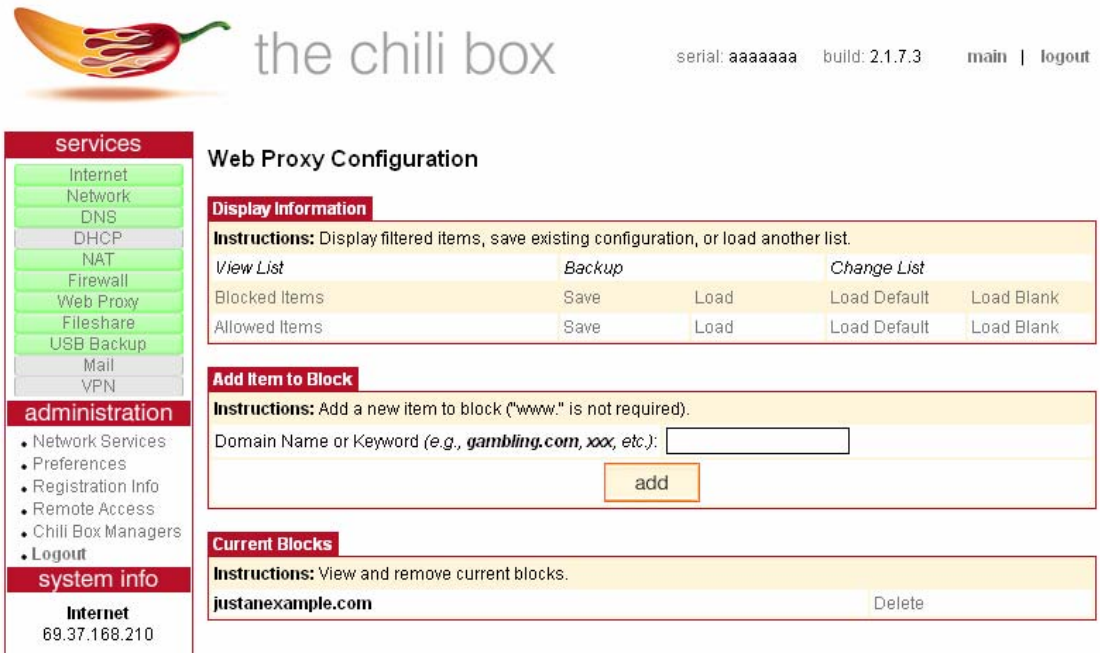
Add Block

You can easily and quickly add items to the “Blocked Items” section by doing the following:

1) Under “Add Item to Block”, enter the domain name or phrase.
2) Click ‘add’.

NOTE: When entering a domain name, “www.” is not required.

After each item has been added, the page will be refreshed and the new entry will appear at the end of the entire listing. If you wish to delete an entry, simply click the “Delete” link to the right. Since there is no confirmation before permanently deleting the block, you may click the ‘Back’ button of your browser if you make a mistake, then re-enter the item.



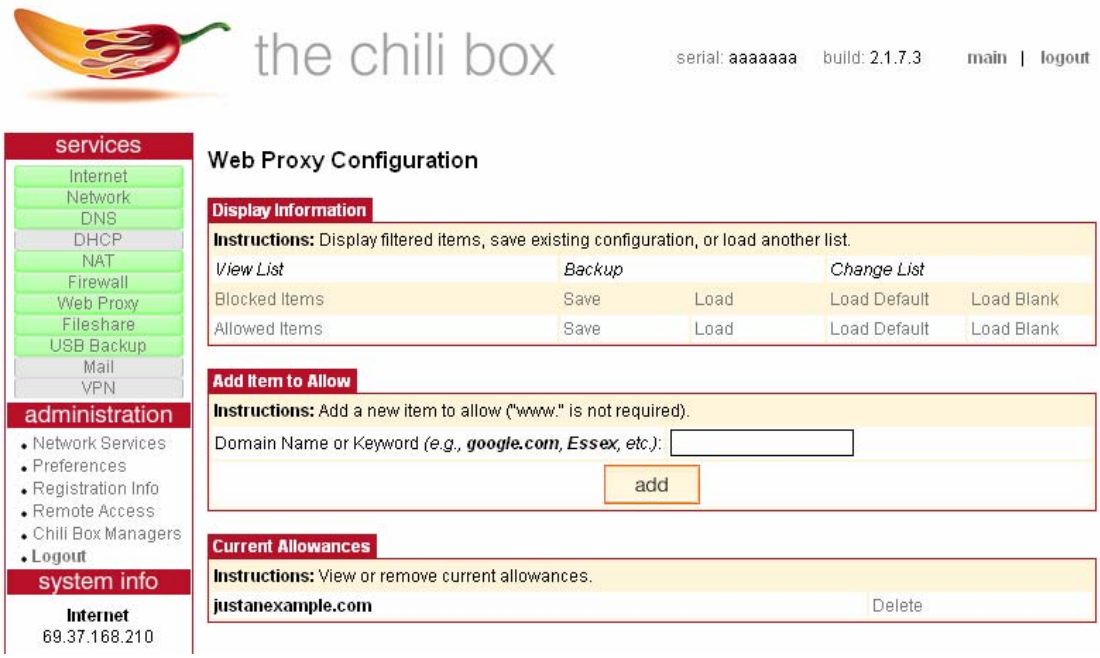
Add Allowance

As with blocking phrases or sites, you can easily and quickly add items to the “Allowed Items” section by doing the following:

1) Under “Add Item to Allow”, enter the domain name or phrase.
2) Click ‘add’.

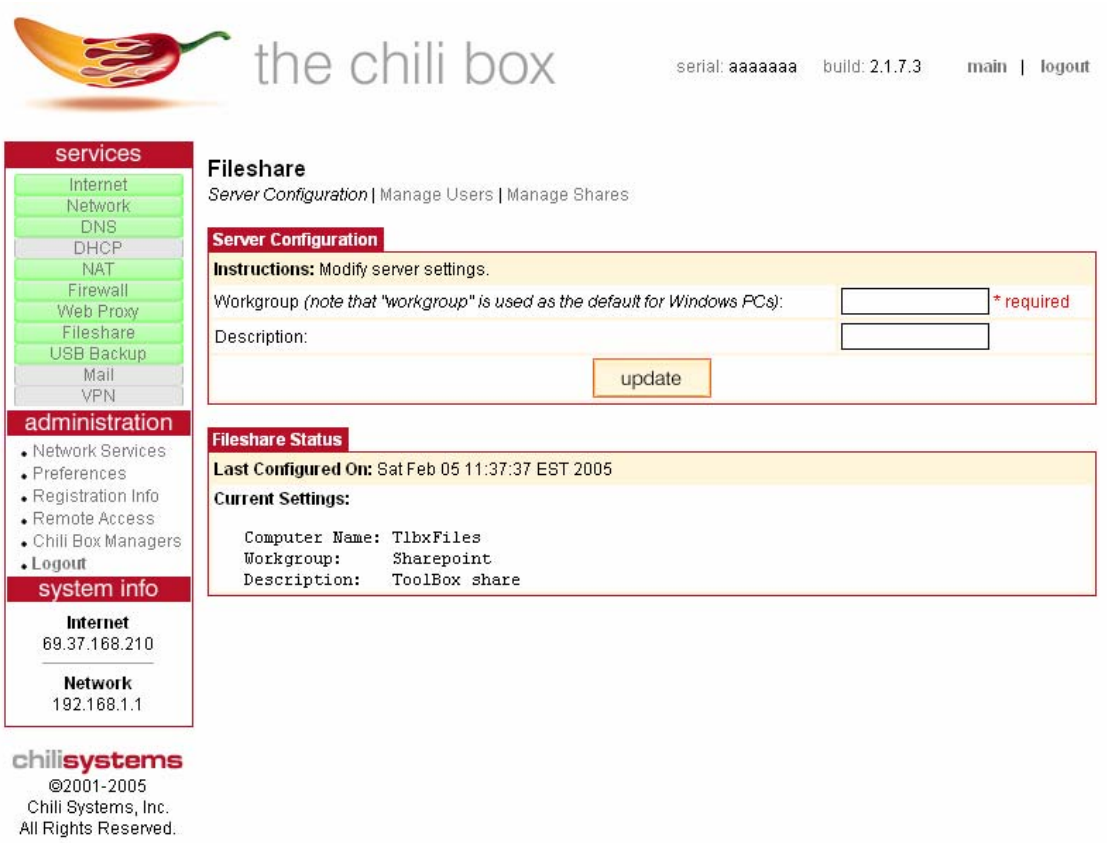
NOTE: When entering a domain name, “www.” is not required.

After each item has been added, the page will be refreshed and the new entry will appear at the bottom of the entire listing. If you wish to delete an entry, simply click the “Delete” link to the right. Since there is no confirmation before permanently deleting the allowance, you may click the ‘Back’ button of your browser if you make a mistake, then re-enter the item.



Fileshare

A fileshare allows a network to have a central location for data, such as photos, videos, MP3s, documents, and so on. Users on the network will have access to the files depending on their usage permissions.



Workgroup – This is the "Share" name of the Fileshare, which is similar to the machine name of a computer on the network.

Description – This is used to describe the Workgroup.

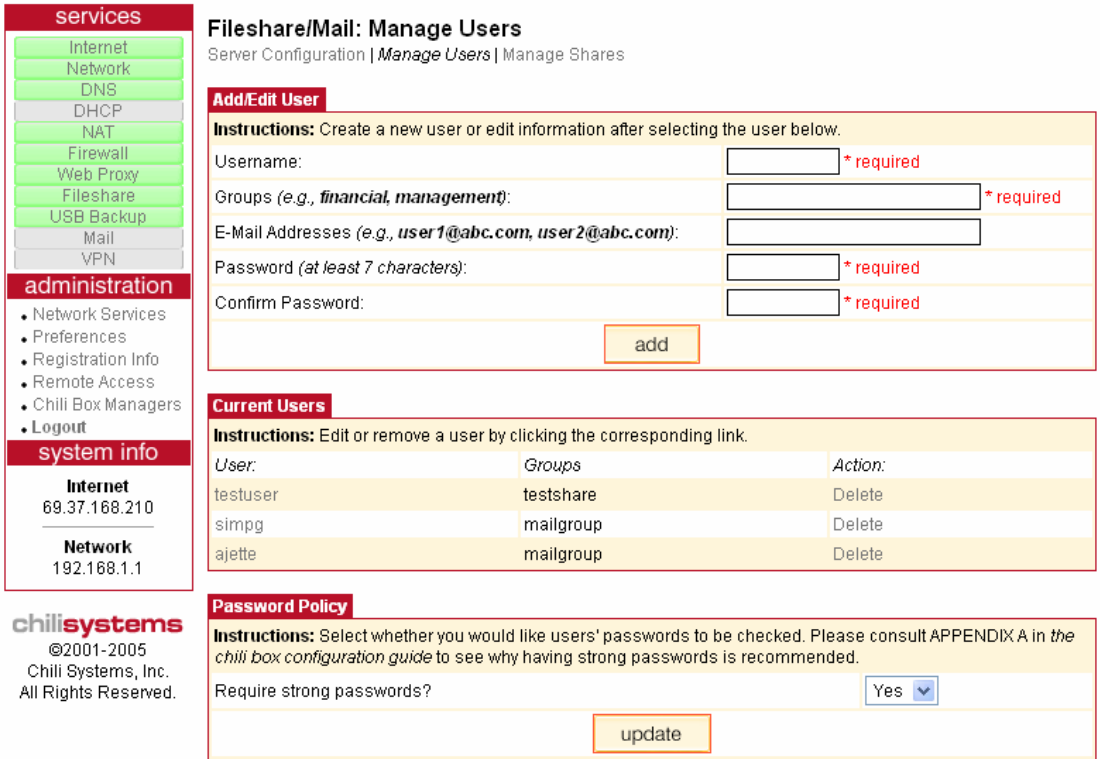
Edit Chili Box Workgroup Name

If you wish to rename the workgroup to be accessed by users on the network, you may do so by following these steps:

1) Under "Workgroup", enter the name.
2) Under "Description", enter the description of the server.
3) Click 'update'.

Manage Users

This section is used to add, modify, and delete users for Fileshare access.



Username – The account name for the user, which will also be used for Mail.

Groups – The group(s) the user is a member of.

E-mail Addresses – The associated e-mail address(es) for the user, which will also be used for Mail.

Password – Enter the password to be used for the user.

Confirm Password – Enter the password again for verification by the chili box.

Add User

To add an account on the Fileshare server, simply do the following:

1) Under, “Add/Edit User”, enter the “Username”.
2) Enter the “Group” (one or many) the user will be a member of.
3) Enter the “E-mail Addresses” that will be directed to the account.
4) Enter the “Password”, then re-enter it in the “Confirm Password” field.
5) Click ‘add’ when finished.

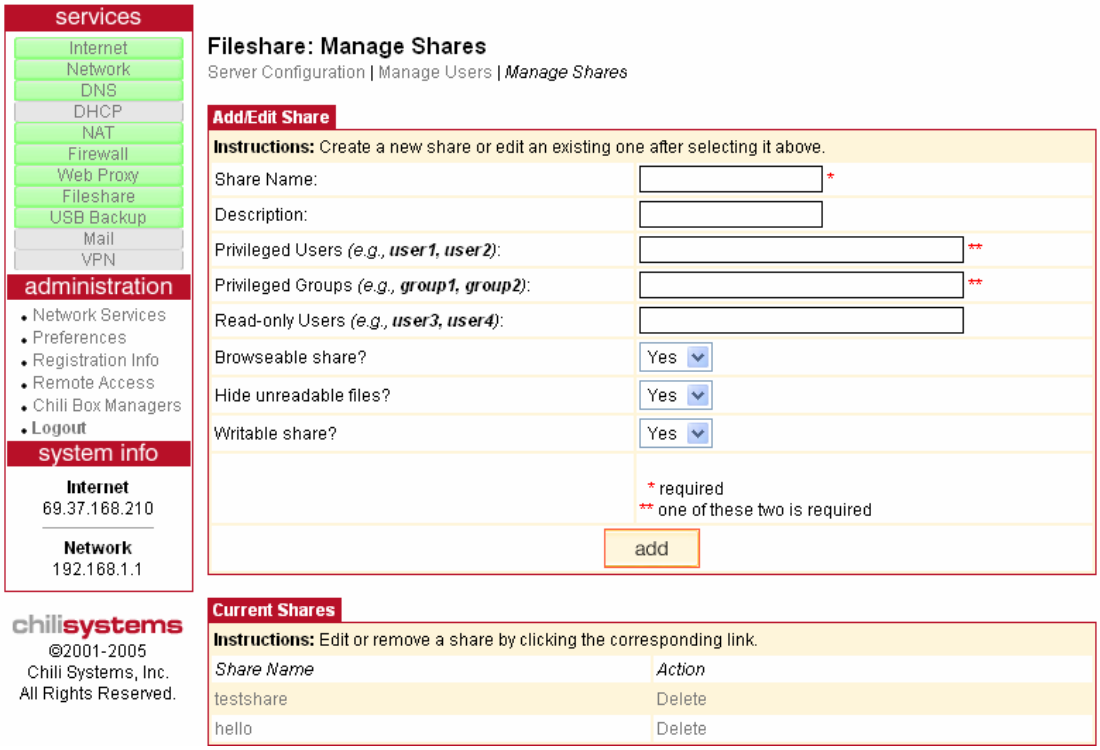
Edit User

To edit an account on the Fileshare server, simply do the following:

1) Under “Current Users”, click the user you wish to edit, which is listed under “User”.
2) At the bottom of the page, under “Add/Edit User”, edit the information you wish to change.
3) You must re-enter it in the “Password” and “Confirm Password” fields.
4) Click ‘add’ when finished.

Manage Shares

This section is used to add, modify, or delete Shares.



Share Name – The name for the Share.

Description – This is used to describe the Share name. It will show up when one selects the Share on the client computer.

Privileged Users – The user(s) who has/have full access rights (read, modify, delete) to the Share.

Privileged Groups – The group(s) that has/have full access rights to the Share.

Read-only Users – The user(s) who has/have limited access rights (read-only) to the Share.

Browseable share? – Used to specify if the Share is capable of being shown without knowing the Share name. If "No" is selected, it will only be accessible by manually entering the information on the client computer.

Hide unreadable files? – Used to specify if system files are to be shown. If "No" is selected, system files will be viewable.

Writable share? – Used to specify if the share can be updated. If "No" is selected, all users would only have read-only access.

Add Share

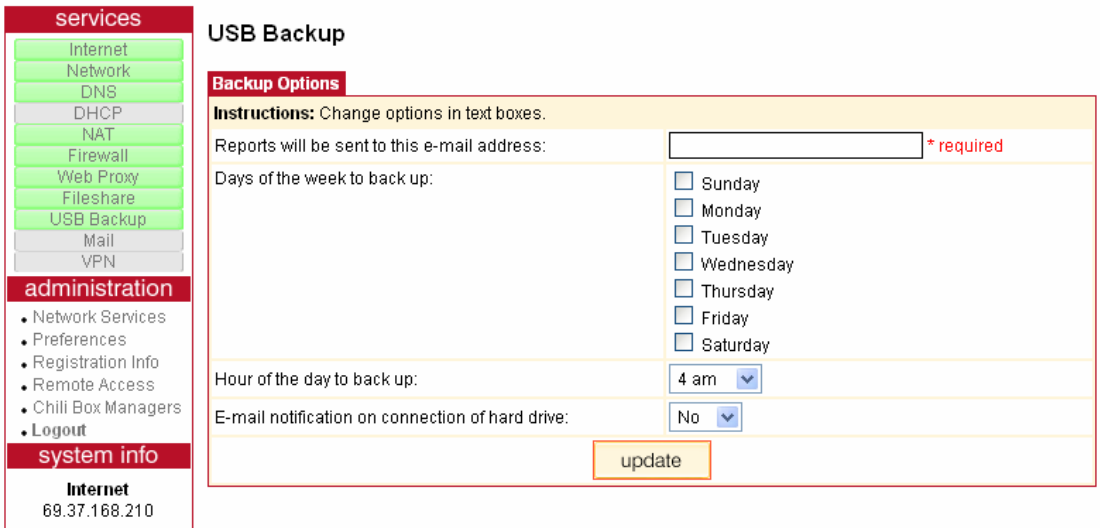
1) Under “Add/Edit Share”, enter the “Share Name” (the name you would like to associate with the Share).
2) Enter the “Description” you would like to use.
3) Enter the “Privileged Users” by entering the usernames, separated by commas.
4) Enter the “Privileged Groups” by entering the usernames, separated by commas.
5) Enter the “Read-only Users” by entering the usernames, separated by commas.
6) Select if you would like it to be a “Browseable Share”.
7) Select if you would like to “Hide Unreadable Files”.
8) Select if you would like it to be a “Writable Share”.
9) Click ‘add’ when finished.

Edit Share

1) Under “Current Shares”, click the share you wish to edit, which is listed under “Share Name”.
2) At the bottom of the page, under “Add/Edit Share”, edit the information you wish to change.
3) Click ‘add’ when finished.

USB Backup

The USB Backup feature on the chili box allows you to fully back up your data from the Fileshare. No longer do you have to be concerned about your data being lost by hardware failure or other causes, such as a fire, since you will be able to easily disconnect the external hard drive to take with you when you leave the location.



Reports will be sent to this e-mail address – Enter the e-mail address to which the reports will be sent. The recipient will receive notices of successful and unsuccessful backups.

Days of the week to back up – Select any or all of the days that you would like the backup to take place.

Hour of the day to back up – Select what time you would like the backup to occur. We recommend selecting an after-hours time, such as very early in the morning or late at night.

E-mail notification on connection of hard drive – Select whether the recipient specified for receiving the reports will get an e-mail when the external hard drive has been connected to the USB port.

Mail

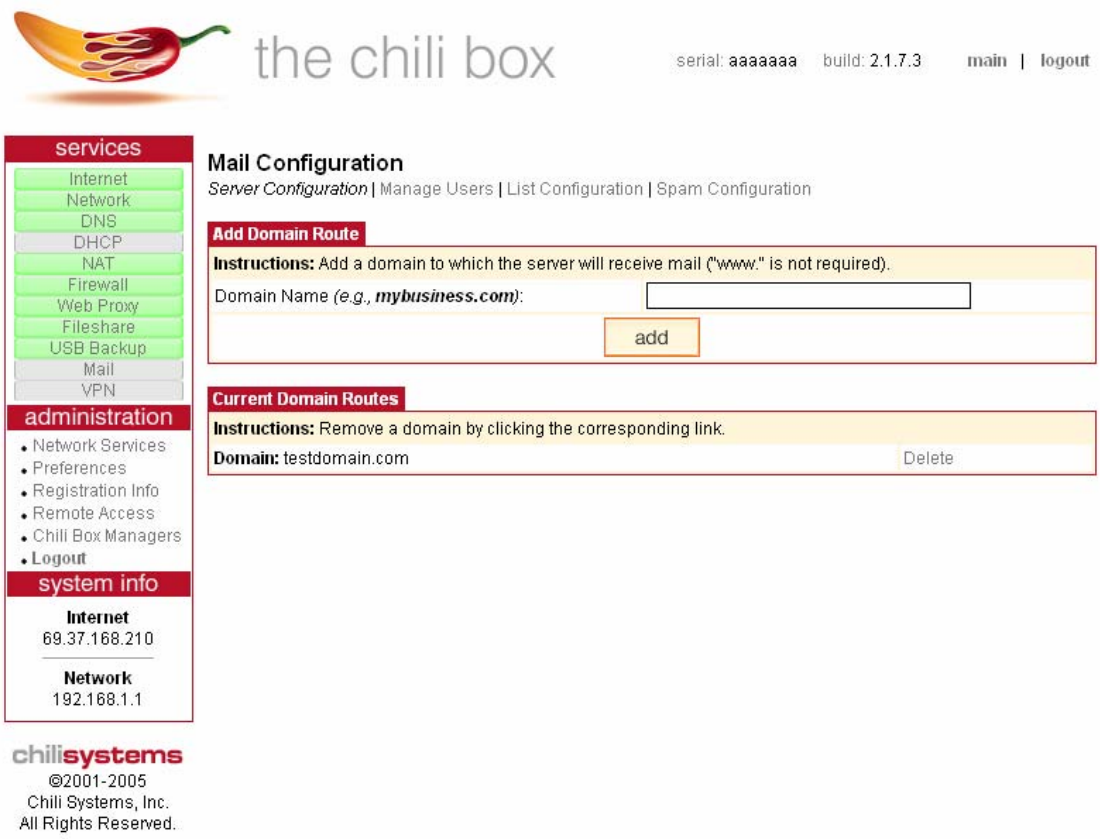
This section allows the capability of full management for Mail services. These include adding a domain name for Mail that the chili box will be responsible for, as well as assigning e-mail accounts, addresses, lists, and configuring the spam setting.

Server Configuration

To add a domain name that the Mail server will be responsible for, simply do the following:

1) At the “Server Configuration” page, under “Add Domain Route” enter the “Domain Name”.
2) Click ‘add’.

NOTE: When entering the domain name, “www.” is not required.



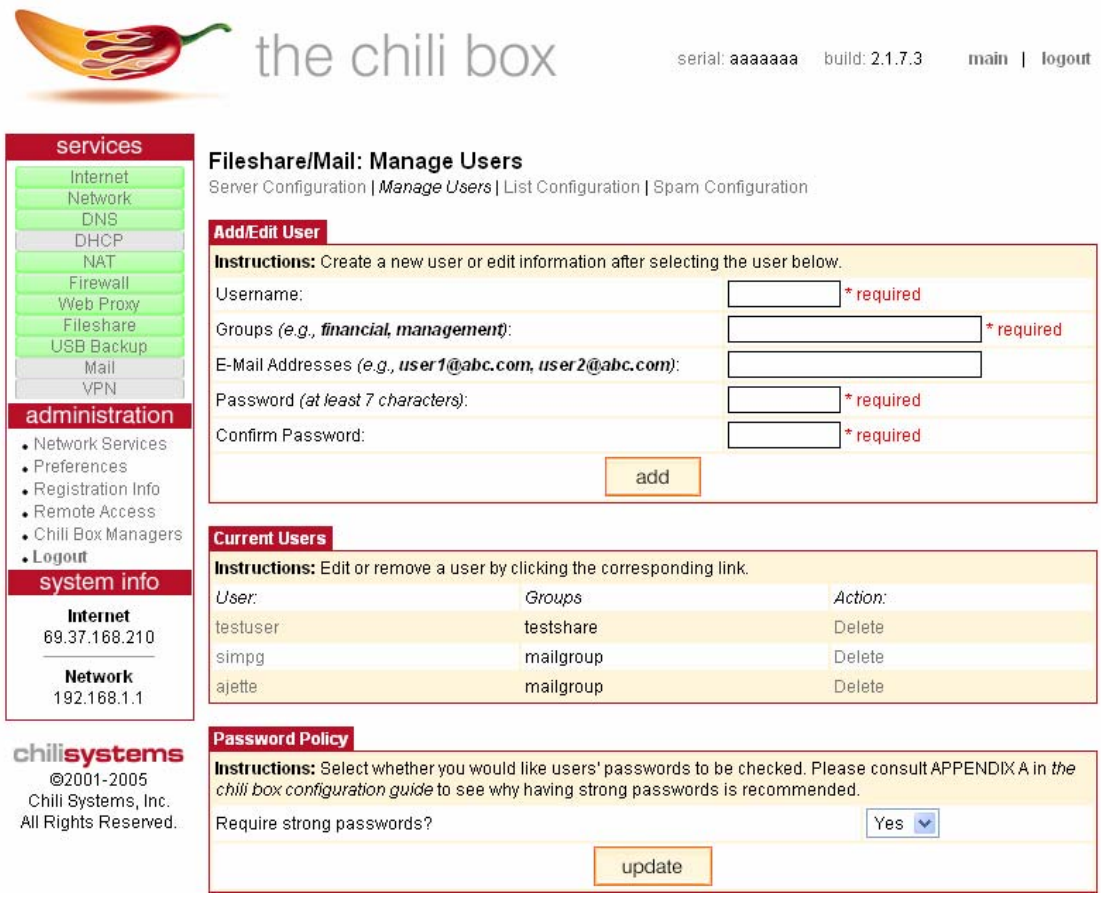
Manage Users

To **add** an e-mail account on the Mail server, simply do the following:

1) At the “Manage Users” page, under “Add/Edit User” enter the “Username”.
2) Enter the “Groups” the user will be a member of.
3) Enter the “E-mail Addresses” that will be directed to the account.
4) Enter the “Password”, then re-enter it in the “Confirm Password” field.
5) Click ‘add’ when finished.

To **edit** an e-mail account on the Mail server, simply do the following:

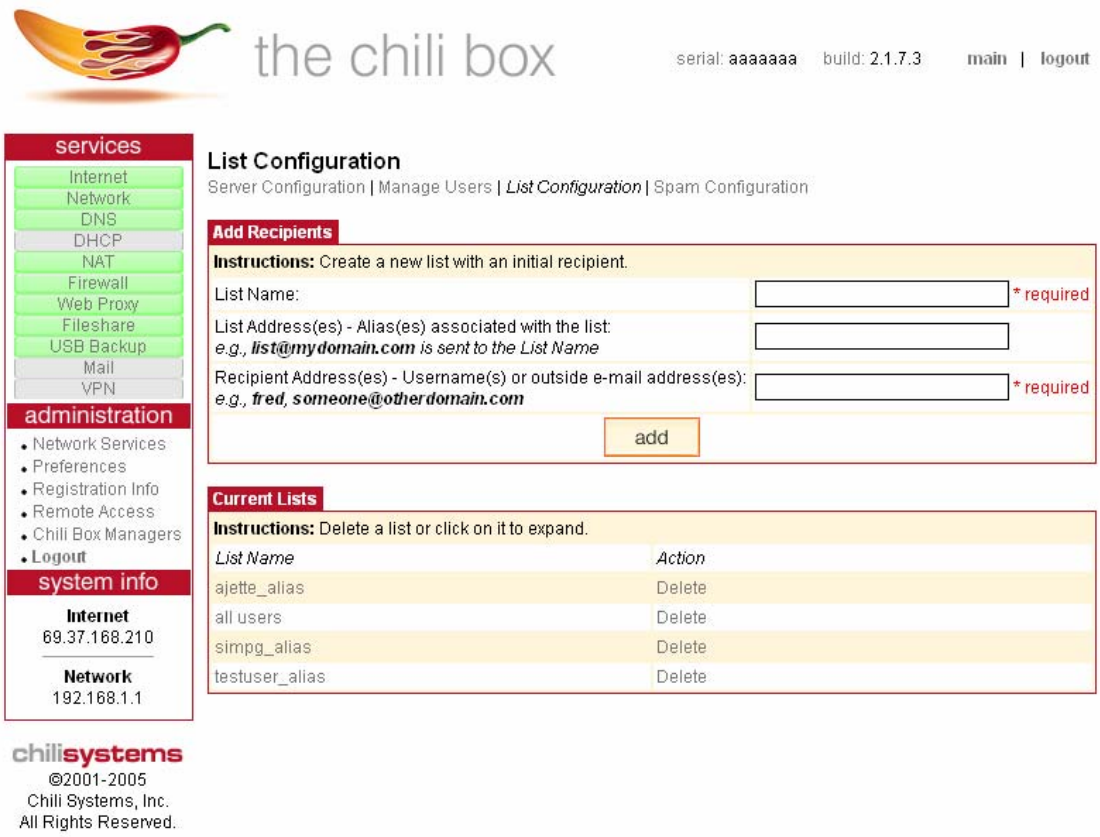
1) Under “Current Users”, click the user you wish to edit, which is listed under “User”
2) At the top of the page, under “Add/Edit User”, edit the information you wish to change.
3) Since the chili box does not store unencrypted passwords, you must re-enter it in the “Password” and “Confirm Password” fields.
4) Click ‘update’ when finished (the ‘add’ button will change).



List Configuration

To add a distribution list that the Mail server will send e-mail to, simply do the following:

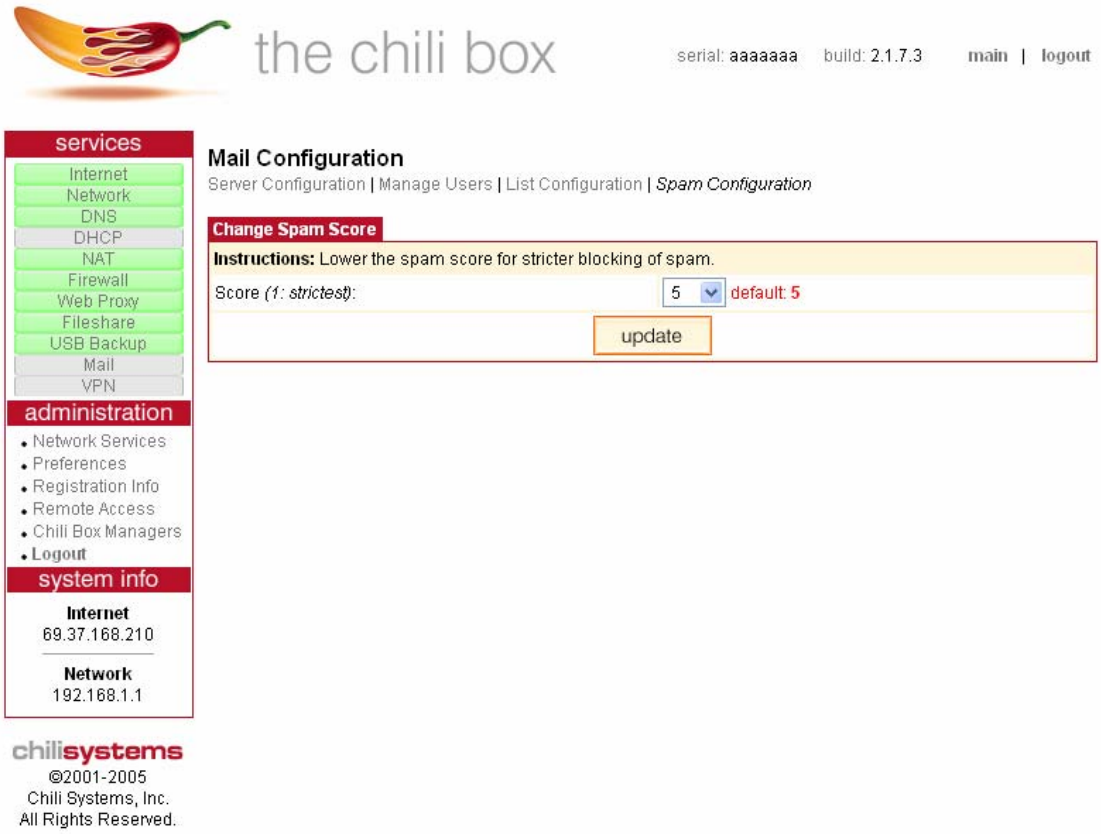
1) At the “List Configuration” page, under “List Name” enter the name to which you would like to refer to the distribution list.
2) Enter the “List Address(es)” for the list. For example, e-mail sent to info@mydomain.com and sales@mydomain.com can both be associated to the list called “request”.
3) Enter the “Recipient Address(es)” for the list. For example, e-mail sent to info@mydomain.com and sales@mydomain.com will go to internal users (e.g., simpg, testuser, etc.) and outside e-mail addresses (e.g., someone@otherdomain.com, bob@somewhere.com, etc.).
4) Click ‘add’.



Spam Configuration

To change the default spam score for stricter blocking of spam received through the Mail server, simply do the following:

1) At the “Spam Configuration” page, under “Change Spam Score” change the “Score”. You may select any number from 1 to 10, with 1 being the strictest (which will filter out the most spam, but may result in false positives) and 10 being the most lenient (a minimal amount of spam will be detected.
2) Click ‘update’ when finished.
3) Since potential spam messages will show up with {Spam?} before the subject, you may create a filter in your mail program to automatically move e-mail determined to be spam to a separate folder (e.g., ‘Junk’ or ‘Deleted Items’). Please refer to your mail program’s Help feature for directions.



VPN

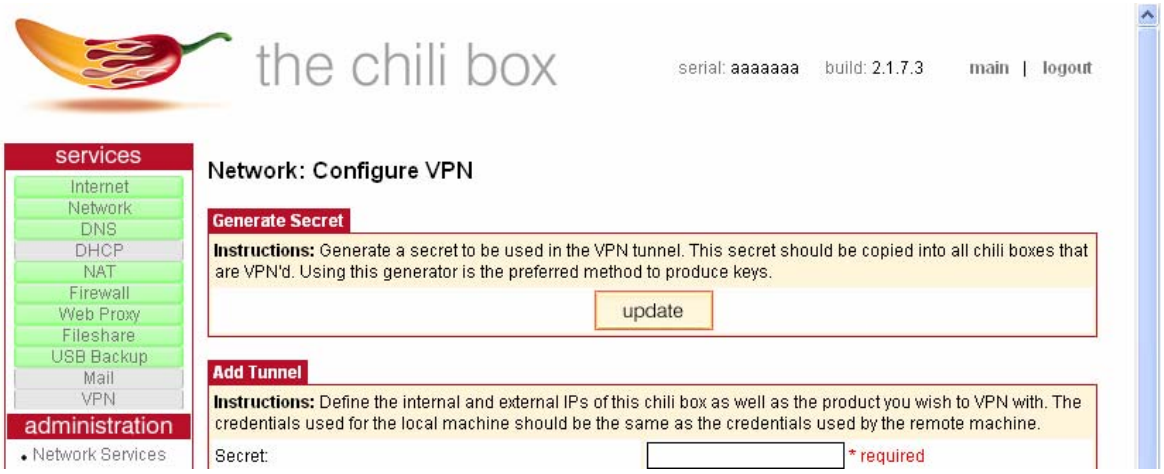
A VPN (Virtual Private Network) allows you to securely connect from one location to another over an encrypted tunnel. This is the preferred method of connecting different locations due to its strong security features. In addition, by using a VPN the locations will appear to be on the same network, even though they may be in different states or even countries.

Generate Secret

To generate a secret for the VPN tunnel, which acts as a key so the two locations can communicate with each other, simply do the following:

1) Under “Generate Secret” click ‘update’.
2) The generated secret will be shown under “Add Tunnel” (under “Secret”).

NOTE: Although you are able to use your own secret, we recommend allowing the chili box to assign one for you. Since it is randomly generated, this is the most secure method.



Add Tunnel

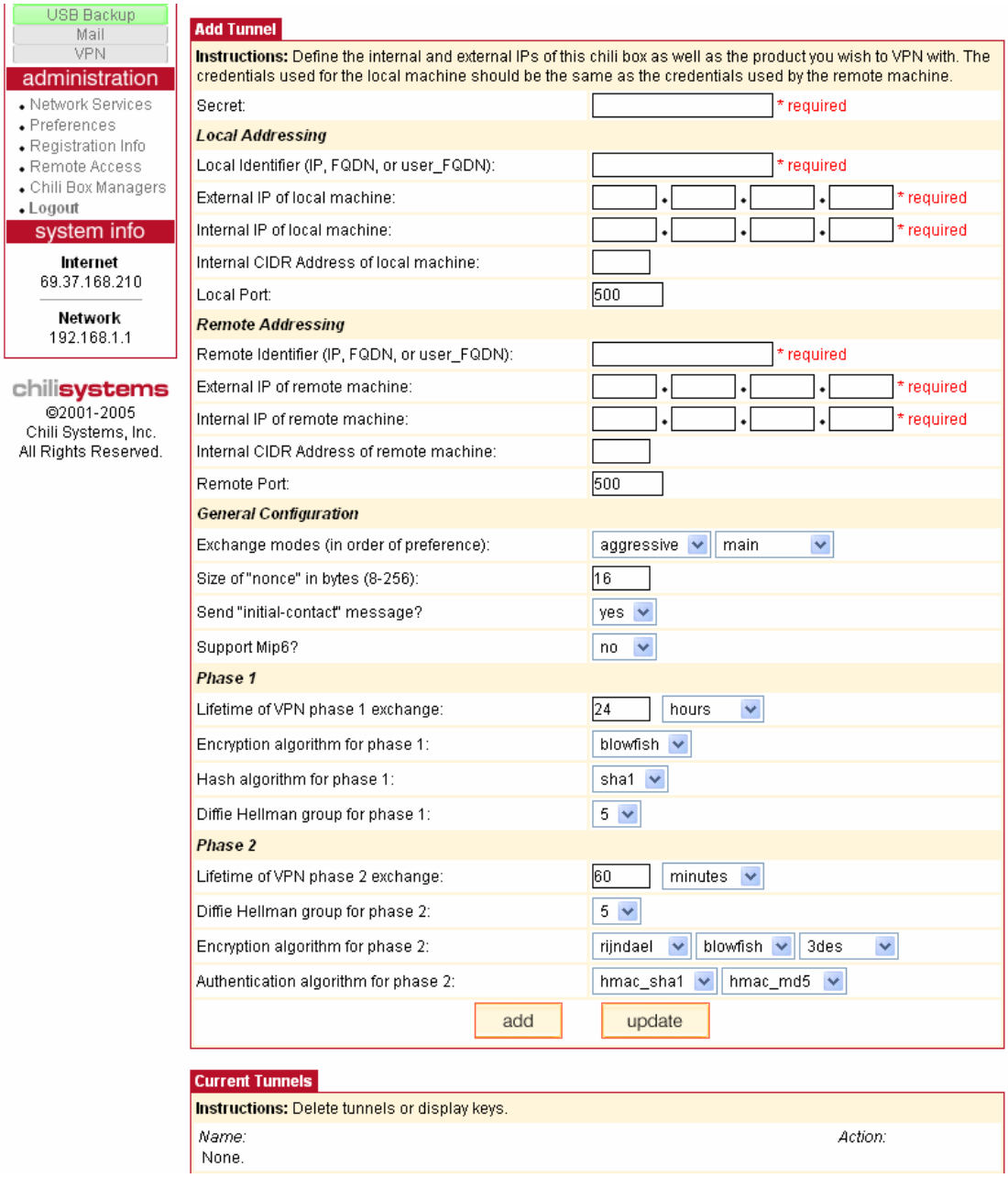
To add a VPN tunnel on the chili box, follow the below steps (see next page for screen shot):

Local Addressing

1) Under “Local Identifier”, enter the IP address or domain name to which you would like to refer to the setup on the current chili box.
2) Enter the external IP of the current chili box under “External IP of local machine” (found in the “system info” box on the left, under “Internet”).
3) Enter the internal IP of the current chili box under “Internal IP of local machine” (found in the “system info” box on the left, under “Network”).
4) Enter the CIDR address for the current chili box, if necessary, under “Internal CIDR Address of local machine”.
5) The default “Local Port” is 500, which may be changed if necessary (it must be the same as the remote port).

Remote Addressing

6) Under “Remote Identifier”, enter the IP address or domain name to which you would like to refer to the setup at the other location (a second chili box or a VPN device).
7) Enter the external IP of the other location under “External IP of remote machine”.
8) Enter the internal IP of the other location under “External IP of remote machine”.
9) Enter the CIDR address for the other location, if necessary, under “Internal CIDR Address of remote machine”.
10) The default “Remote Port” is 500, which may be changed if necessary (it must be the same as the local port).
11) If you do not need to specify any settings under *General Configuration*, *Phase 1*, or *Phase 2* you may click ‘add’. If you need to make additional changes, update the configuration then click ‘add’.



Edit Tunnel

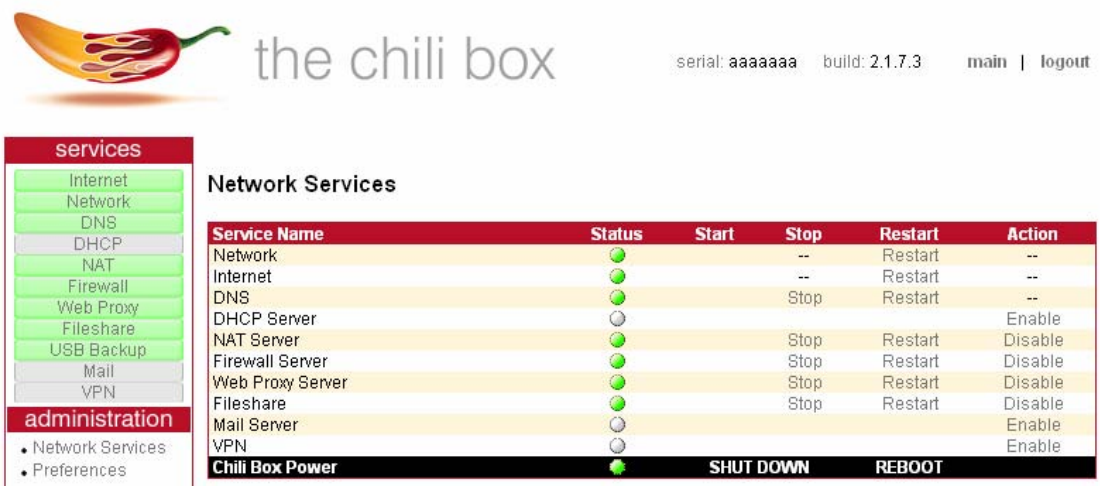
To edit a VPN tunnel on the chili box, follow the below steps:

1) Under “Current Tunnels”, click the VPN tunnel you wish to edit (the External IP of the remote machine is shown).
2) When the current tunnel’s information is shown, edit the fields you wish to change (e.g., “External IP of remote machine”).
3) Click ‘update’ when finished.

Network Services

The purpose of this section is to display the status of all services of the chili box and allow the capability to start, stop, restart, and disable the available services. If a message is displayed to restart a service after making a configuration change, it is done here.

NOTE: If any of the below services are not running on your chili box, it is likely that the services are not being used.



Stop, Restart, or Disable Service

NOTE: JavaScript must be enabled so the below options in red can be stopped or restarted:

Service Name	Stop	Restart	Action
Internet	--	Restart	--
Network	--	Restart	--
DNS	Stop	Restart	--
DHCP Server	Stop	Restart	Disable
NAT Server	Stop	Restart	Disable
Firewall Server	Stop	Restart	Disable
Web Proxy Server	N/A	N/A	Disable
Fileshare	Stop	Restart	Disable
Mail Server	N/A	N/A	Disable
VPN	--	--	Disable
Chili Box Power	SHUT DOWN	REBOOT	

The condition of a service can be changed at any time. Please note that those with "--" as their choices are not available. This is done so no required service is inadvertently stopped.

How to Restart the Chili Box

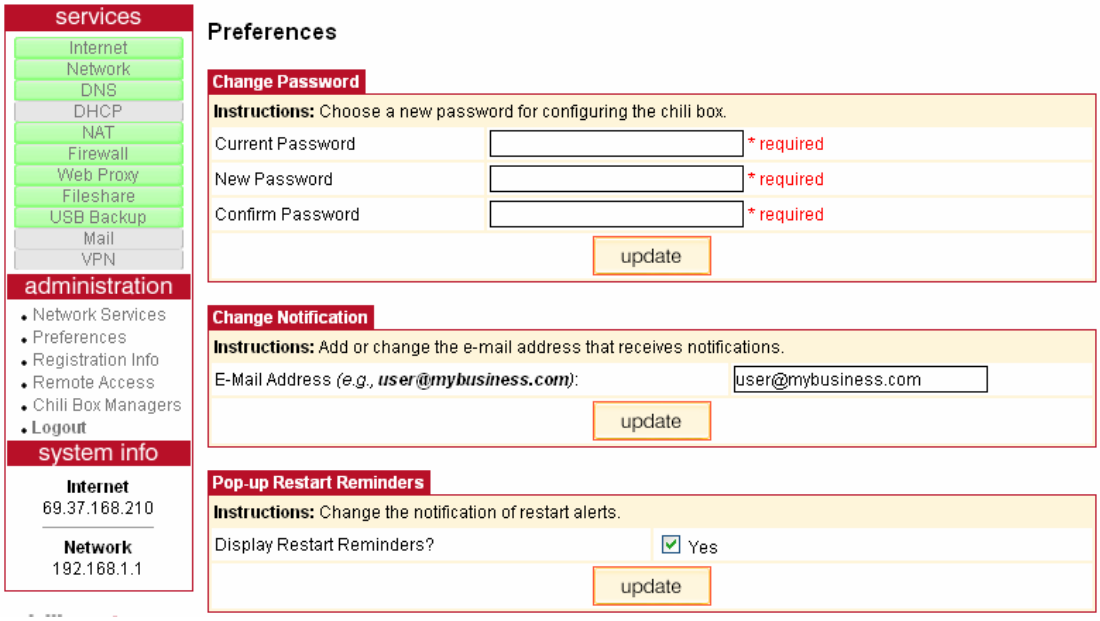
If you would like to restart the chili box, please follow these directions. It is very important to restart the chili box according to these steps, as potential data loss or connectivity problems may occur if they are not followed.

1) After you have logged in successfully, click the “Network Services” link in the left navigation bar.
2) On the **Chili Box Power** row, click the **REBOOT** link to restart the chili box. When you see the confirmation pop-up, click ‘OK’ to confirm the selected action.
3) After the chili box has been successfully restarted, you may log in again to verify everything is working correctly.

NOTE: To turn off the chili box, press the power button and release it. ***DO NOT KEEP THE POWER BUTTON PRESSED.*** *Wait for both LEDs to turn off, which may take up to a minute.*

Preferences

If you would like to change your password, update the e-mail address that receives notifications, and enable/disable pop-up restart reminders, it is done in this section.



Change Password

To change the password for the current user, simply follow the below directions:

1) Enter the current password under “Current Password” and the new password under “New Password”. Re-enter it in the “Confirm Password” field.
2) Click ‘update’ to initiate the change.

Change Notification

To add/edit the e-mail address that receives notifications, follow these steps:

1) Enter the e-mail address under “E-mail Address”.
2) Click ‘update’ for the change to take effect.

Pop-up Restart Reminders

To change the option to have a pop-up dialog box appear when a service requires a restart for the changes to occur, follow the below directions:

1) If you would like the prompt to appear, check “Yes” under “Display Restart Reminders?”; otherwise, make sure the box is NOT checked.
2) Click ‘update’ to save the setting.

Remote Access

This page will allow you to change the option of managing the GUI from a remote location. For instance, you may wish to change certain settings on the chili box when you are away from home or the office.

Remote Administration

To modify the ability to remotely access the GUI, follow these steps:

1) If you would like the ability to manage the box from the outside, check “Yes” under “Allow remote administration?”; otherwise, make sure the box is NOT checked.
2) Click ‘update’ to save the setting.

Enable Chili Systems Technical Support

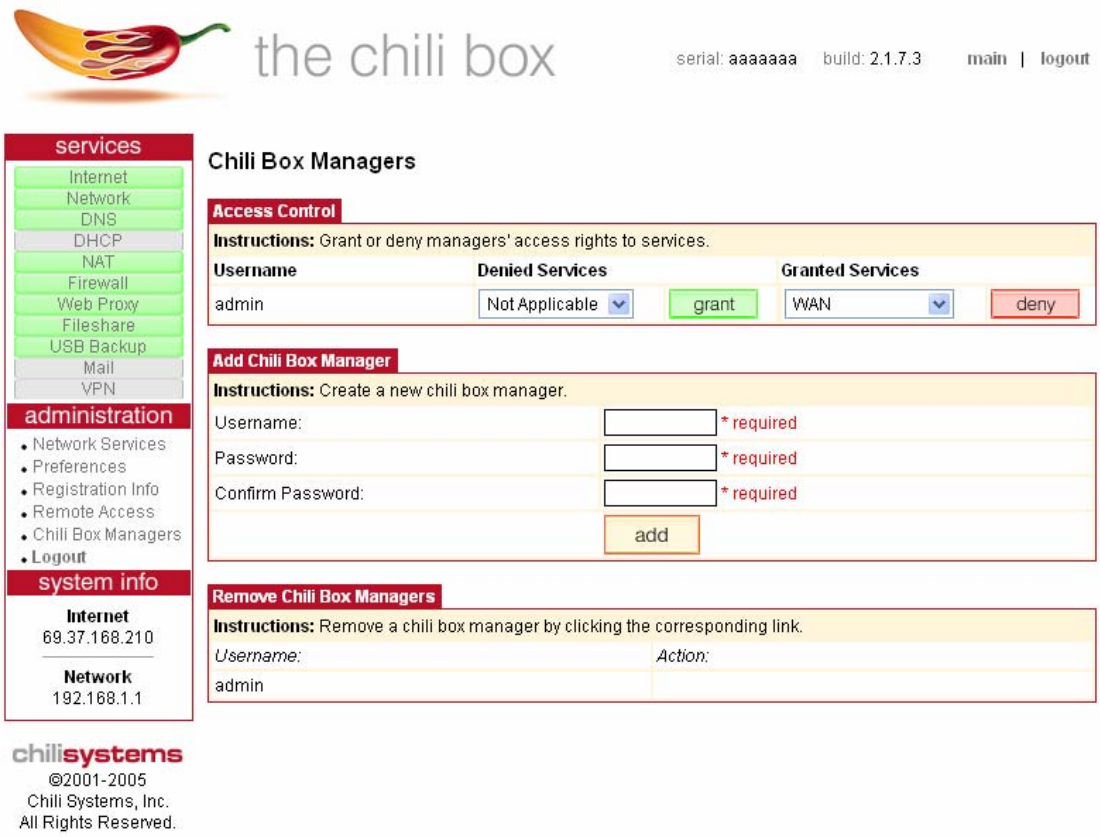
While you are speaking with a technical support representative, you have the ability to allow him/her to connect to your chili box from the back-end. By checking this option, the tech will be more likely to solve your problem in a timely and efficient manner:

1) If you would like to allow a representative to connect to your chili box from the back-end, check “Yes” under “Allow technical support?”; otherwise, make sure the box is NOT checked.
2) Click ‘update’ to save the setting.

Chili Box Managers

If you would like to allow privileged users to have access to the chili box GUI, it is done in this section. You can easily change the services each chili box Manager has access to by selecting the appropriate service and clicking the corresponding button ('Grant' or 'Deny').

NOTE: When logged in as "admin", it is possible to grant or deny existing services for the "admin" account. Although you may always correct any mistake, make the changes carefully.



Add Chili Box Manager

To allow access for a certain user, simply follow the below directions. If the user has a Mail or Fileshare account, the same username may be used, but it is completely separate from the mentioned services.

1) Under "Add chili box Manager", enter the "Username".
2) Enter the "Password", then re-enter it in the "Confirm Password" field.
3) Click 'add'. By default, all services are denied. You may grant or deny services by selecting each option then clicking the corresponding button ('Grant' or 'Deny').

APPENDIX A: How to Choose a Password

chili box security

Strong passwords—ones that are at least eight characters long, include both letters and two numbers as well as one special character or symbol—for chili box managers are an absolute necessity. We believe in setting a high standard of security, but unauthorized changes can occur if someone can guess the password of a manager's account. Using the Secure Sockets Layer (SSL), the password is sent encrypted, but "brute force" techniques may still be used to discover the password.

An attacker may attempt to log into the remote administration as an administrator and try different passwords. Although we have considered locking this type of account, it will only cause valid administrators to be locked out by attackers. Failed password attempts are logged, but with enough attempts the password may be uncovered.

employee security

For users on the chili box that are set up to use services, passwords are also extremely important. If an employee's password is acquired, his or her e-mails can be read or personal files on the Fileshare can be altered or stolen. Other problems can arise, such as filling up the chili box hard drive(s) so that no more space can be used by employees.

about password attacks

Common password attacks are accomplished using dictionary files, which contain common words and password combinations such as "passwd" or "changeme". It is also trivial to write a program that will try random words in the dictionary and append or prepend numbers to them (e.g., "cactus1" or "45cactus"). The program could be expanded to also substitute numbers or symbols for letters, or to shorten words (e.g., "apple" would become "Apple" or "appLe", or even perform other attempts like "app!" or "appl3"). Passwords of this nature can and eventually will be cracked. An extremely secure password is more than 8 characters long and comprised of random numbers, letters, and symbols (e.g., "8gh.Zh;q*1f"). Since we advocate not writing down passwords, they should be made easy to remember yet still hard to break. Below are some guidelines to choose this type of password.

1) Select a phrase, such as "I enjoy old blue cars from Ford or Chrysler"
2) Attempt to modify real words into imaginary words, such as "IeObCfFoC"
3) You can then place the words together, or separate them using special characters, or both. An example of this could be "IeO,bC;fFoC". Certainly make it as easy to remember as possible.
4) At the end, substitute some numbers in and possibly capitalize. The final password becomes "Ie0,bC;fF0C". Though it looks rather complicated, it is still quite similar to "I enjoy old blue cars" and is near impossible to guess. The password could surely be a little easier, but this is just an example. Other examples follow:

   - "home sweet home is the place to be" becomes "hSh1+ptB"
   - "I love relaxing on the weekends" becomes "I1r$0tW"